Amendments to the claims,
Listing of all claims pursuant to 37 CFR 1.121(c)

This listing of claims will replace all prior versions, and listings, of claims in the application:

What is claimed is:

1. (Currently amended) A method for protecting a computer from security breaches involving devices that may be attached to the computer, the method comprising:

when a device is first attached to the computer, requiring user-provided information for authorizing the device;

based on the user-provided information, ~~specifying~~ storing authorization information indicating whether or not that the device is allowed to communicate with the computer;

detecting detachment of the device from the computer;

updating the authorization information to indicate that the device is no longer authorized to communicate with the computer; and

upon reattachment of the device, blocking communication with the device while the device remains unauthorized, thereby preventing a security breach involving the device.

2. (Original) The method of claim 1, wherein said specifying step includes: specifying a password for authorizing the device.

3. (Original) The method of claim 1, wherein said specifying step includes: specifying at least one user with sufficient privileges to authorize the device.

4. (Original) The method of claim 1, wherein the device is attached to the computer via a port.

5. (Original) The method of claim 4, wherein the port is a selected one of a USB port, an RS-232 port, a parallel port, a SCSI port, and an IEEE 1394 port.

6. (Original) The method of claim 1, wherein said device comprises an input device and wherein said blocking step includes blocking input from the input device.

7. (Original) The method of claim 6, wherein said input device is a keyboard device.

8. (Original) The method of claim 7, further comprising:

upon reattachment of the keyboard device, trapping keystrokes from the keyboard device.

9. (Original) The method of claim 8, further comprising:

determining whether keystrokes trapped from the keyboard comprise a password that may be used to authorize the device.

10. (Original) The method of claim 1, wherein said device comprises a detachable storage device and wherein said blocking step includes blocking any data stream from the storage device.

11. (Original) The method of claim 1, wherein said blocking step includes:

blocking communication from the computer to the device while the device remains unauthorized.

12. (Original) The method of claim 1, further comprising:

receiving input authorizing the device; and thereafter

allowing communication with the device.

13. (Original) The method of claim 12, wherein the input comprises password input from an authorized user.

14. (Original) The method of claim 1, further comprising:

upon detecting detachment of the device from the computer, generating an alert that reports the detachment.

15. (Original) The method of claim 14, wherein the alert is automatically transmitted to a system administrator.

16. (Original) The method of claim 14, wherein the alert is automatically transmitted to a remote administration module operating on a different computer.

17. (Original) The method of claim 1, further comprising:
receiving authorization from a remote administration module; and thereafter
allowing communication with the device.

18. (Original) The method of claim 1, wherein said specifying step includes:
specifying an operating system hook that allows attachment and detachment of devices to be detected.

19. (Original) The method of claim 1, wherein said updating step includes:
updating the authorization information to indicate that the device is currently untrusted.

20. (Original) The method of claim 1, wherein said updating step includes:
treating the detachment as a security breach and blocking communication with a network node that the computer resides on.

21. (Original) A computer-readable medium having processor-executable instructions for performing the method of claim 1.

22. (Original) A downloadable set of processor-executable instructions for performing the method of claim 1.

23. (Currently amended) A system for protecting a computer from security

breaches involving devices that may be attached to the computer, the system comprising:

an agent module for specifying, in response to user-provided information, authorization information indicating ~~that~~ whether or not a device is allowed to communicate with the computer when the device is first attached to the computer; for detecting detachment of the device from the computer; and for updating the authorization information to indicate that the device is no longer authorized to communicate with the computer; and

a filter module for blocking communication with the device while the device remains unauthorized, thereby preventing a security breach involving the device.

24. (Original) The system of claim 23, wherein the agent module includes:

program logic for specifying a password for authorizing the device.

25. (Original) The system of claim 23, wherein the agent module includes:

program logic for specifying at least one user with sufficient privileges to authorize the device.

26. (Original) The system of claim 23, wherein the device is attached to the computer via a port.

27. (Original) The system of claim 26, wherein the port is a selected one of a USB port, an RS-232 port, a parallel port, a SCSI port, and an IEEE 1394 port.

28. (Original) The system of claim 23, wherein said device comprises an input device and wherein the filter module includes program logic for blocking input from the input device.

29. (Original) The system of claim 28, wherein said input device is a keyboard device.

30. (Original) The system of claim 29, wherein said filter module includes:

program logic for trapping keystrokes from the keyboard device.

31. (Currently amended) The system of claim 30, wherein said filter module further includes:

program ~~logicfor~~ logic for determining whether keystrokes trapped from the keyboard comprise a password that may be used to authorize the device.

32. (Original) The system of claim 23, wherein said device comprises a detachable storage device and wherein the filter module includes program logic for blocking any data stream from the storage device.

33. (Currently amended) The system of claim 23, wherein the filter module includes:

program ~~logicfor~~ logic for blocking communication from the computer to the device while the device remains unauthorized.

34. (Currently amended) The system of claim 23, wherein said modules further comprise:

program ~~logicfor~~ logic for receiving input authorizing the device, and thereafter

program ~~logicfor~~ logic for allowing communication with the device.

35. (Original) The system of claim 34, wherein the input comprises password input from an authorized user.

36. (Currently amended) The system of claim 23, wherein said agent module further comprises:

program ~~logicfor~~ logic for generating an alert that reports the detachment.

37. (Original) The system of claim 36, wherein the alert is automatically transmitted to a system administrator.

38. (Original) The system of claim 36, wherein the alert is automatically transmitted to a remote administration module operating on a different computer.

39. (Currently amended) The system of claim 23, wherein said modules further comprises:

program ~~logicfor~~ logic for receiving receiving authorization from a remote administration module; and thereafter

program ~~logicfor~~ logic for allowing communication with the device.

40. (Currently amended) The system of claim 23, wherein the agent module includes:

program ~~logicfor~~ logic for specifying an operating system hook that allows attachment and detachment of devices to be detected.

41. (Currently amended) The system of claim 23, wherein the agent module includes:

program ~~logicfor~~ logic for updating the authorization information to indicate that the device is currently untrusted.

42. (Currently amended) The system of claim 23, wherein the agent module includes:

program ~~logicfor~~ logic for treating the detachment as a security breach and blocking communication with a network node that the computer resides on.

43. (Currently amended) A method for securing a computer from security breaches involving peripheral devices, the method comprising:

specifying a password to be supplied by a user for authorizing a peripheral device to communicate with the computer;

detecting each attachment of the peripheral device to the computer;

upon each attachment, blocking communications with the peripheral device until the password is supplied again by the user; and if the password is supplied, permitting the peripheral device to communicate with the computer.

44. (Original) The method of claim 43, wherein said specifying step includes:

specifying at least one user with sufficient privileges to authorize the peripheral device.

45. (Original) The method of claim 43, wherein the peripheral device is attached to the computer via a port.

46. (Original) The method of claim 43, wherein said peripheral device comprises an input device and wherein said blocking step includes blocking input from the input device.

47. (Original) The method of claim 46, wherein said input device is a keyboard device.

48. (Original) The method of claim 47, further comprising:

upon reattachment of the keyboard device, trapping keystrokes from the keyboard device.

49. (Original) The method of claim 48, further comprising:

determining whether keystrokes trapped from the keyboard comprise a password that may be used to authorize the device.

50. (Original) The method of claim 43, wherein said blocking step includes:

blocking communication from the computer to the peripheral device while the peripheral device remains unauthorized.

51. (Original) The method of claim 43, further comprising:

upon any detachment of the peripheral device from the computer, generating an alert that reports the detachment.

52. (Original) The method of claim 51, wherein the alert is automatically transmitted to a system administrator.

53. (Original) The method of claim 51, wherein the alert is automatically transmitted to a remote administration module operating on a different computer.

54. (Original) The method of claim 43, further comprising:

receiving the password from a remote administration module; and thereafter allowing communication with the peripheral device.

55. (Original) The method of claim 43, wherein said specifying step includes:

specifying an operating system hook that allows attachment and detachment of peripheral devices to be detected.

56. (Original) The method of claim 43, further comprising:

treating any detachment of the peripheral device as a security breach and blocking communication with a network node that the computer resides on.

57. (Original) A computer-readable medium having processor-executable instructions for performing the method of claim 43.

58. (Original) A downloadable set of processor-executable instructions for performing the method of claim 43.